REMARKS/ARGUMENTS

This submission is in response to the Final Office Action mailed May 28, 2008. Claims 1, 2, 4-8, and 15-23 were pending and examined. No claims have been amended, canceled, or added. Accordingly, claims 1, 2, 4-8, and 15-23 remain pending in the present application after entry of this submission. Reconsideration of the rejected claims is respectfully requested.

Examiner Interview

Applicants would like to thank Examiner Dada for the telephonic interview regarding this application conducted on July 22, 2008. Applicants' independent claim 1 was discussed in light of Rayes et al. (U.S. Patent No. 7,234,163, hereinafter "Rayes") and Iyer et al. (U.S. Publication No. 2005/0254474, hereinafter "Iyer"). Further, Applicants' independent claim 20 was discussed in light of Doyle (U.S. Patent No. 7,134,012, hereinafter "Doyle"). In particular, distinctions between the claims and the references were discussed.

At the interview, the Examiner indicated that further study would be required to fully consider Applicants' arguments. The following remarks reflect the substance of the discussion.

Allowable Subject Matter

Claim 21 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Applicants appreciate the indication of allowable subject matter in claim 21. However, as discussed in detail below, Applicants submit that independent claim 1, upon which claim 21 depends, is also allowable over the cited prior art.

35 U.S.C. §103 Rejection of Claims 1, 2, 4-8, 15-19, 22, and 23

Claims 1, 2, 4-8, 15-19, 22, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Rayes in view of Iyer. Applicants respectfully traverse the rejection.

Applicants' independent claim 1 recites a method for detecting ARP spoofing in a computer network, the method comprising:

> receiving a data packet at an ARP collector, wherein the data packet is generated by a first device on the network, and wherein the data packet includes information from an ARP reply received at the first device from a second device on the network, the information including a MAC address of the second device and an IP address given as a source IP address of the second device in the ARP reply; and
>
> analyzing at least one association in a database accessible to the ARP collector to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association, and wherein the at least one association includes a MAC address that is identical to the MAC address included in the data packet.
>
> (Applicants' independent claim 1, in part, emphasis added).

Applicant submit that the above-recited features of claim 1 are not taught or suggested by Rayes or Iyer, considered individually or in combination. For example, Rayes and Iyer fail to teach or suggest "analyzing… to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association" as recited in claim 1.

The Office Action concedes that Rayes does not teach the claimed feature of "wherein the analyzing is based on a time associated with the at least one association." However, the Office Action alleges that this feature is shown in Iyer at paragraph 93. (Office Action: pg. 3). Applicants respectfully disagree.

Iyer is directed to an "air monitor" configured to monitor and enforce various policies in a wireless network. (Iyer: Abstract). The cited section of Iyer describes one type of policy enforcement operation wherein the air monitor detects rogue wireless stations that are impersonating valid wireless stations. This is performed by detecting whether the same MAC address is associated with two different wireless stations at the same time. (Iyer: para. 93).

Applicants submit that this section of Iyer does not teach anything about "analyzing… to determine whether ARP spoofing occurs, wherein the analyzing is based on a time associated with the at least one association" as recited in claim 1. As best understood, the Office Action construes the act of detecting whether the same MAC address is associated with two wireless stations at the same time, as described in Iyer, as corresponding to the time-based analysis recited in claim 1. However, the detection described in Iyer is merely used to determine whether MAC address spoofing (or impersonation) occurs (*i.e.*, whether one network device is using the same MAC address as another network device). In contrast, claim 1 specifically recites that the time-based analysis recited therein is used "to determine whether ARP spoofing occurs" (*i.e.*, whether a rogue entity is sending a spoofed ARP reply in response to an ARP request). Applicants submit that the detection of MAC address spoofing, as described in Iyer, is substantially different from the detection of ARP spoofing, as recited in claim 1. Accordingly, the cited section of Iyer fails to teach or suggest "analyzing… to determined whether ARP spoofing occurs, wherein the analyzing based on a time associated with the at least one association" recited in claim 1. (Emphasis added).

Further, Applicants submit that the cited section of Iyer fails to teach or suggest a "time associated with the at least one association" as recited in claim 1. While the cited section does describe an association between a MAC address and a wireless station, nowhere does Iyer teach or suggest that this MAC address-wireless station association is necessarily associated with a specific time. As discussed above, Iyer merely states that an air monitor may detect whether two wireless stations are associated with the same MAC address at the same time. Accordingly, in order to perform this detection, the air monitor of Iyer need only query the MAC addresses of the two wireless stations substantially simultaneously; the air monitor does not need to reference or store any specific time for a given MAC address-wireless station pairing. Thus, Iyer fails to teach or suggest a "time associated with the at least one association" as recited in claim 1.

Further, Applicants note that the "at least one association" in the phrase "time associated with the at least one association" is qualified by other clauses in claim 1. For example, the "analyzing…" step of claim 1 recites that the "at least one association" is stored "in a database accessible to the ARP collector," and "includes a MAC address that is identical to the MAC address included in the data packet." Accordingly, only associations that (1) are stored in a database of an ARP collector, and (2) have a MAC address identical to the MAC address in the recited data packet of claim 1, are relevant in teaching the "at least one association" that is associated with a time in claim 1. Applicants submit that Iyer does not teach or suggest any type of association that fits this description. For example, nowhere does Iyer teach or suggest that the MAC address-wireless station associations described therein exhibit characteristics (1) and/or (2). For at least this additional reason, Iyer cannot be properly construed as teaching or suggesting a "time associated with the at least one association" as recited in claim 1. (Emphasis added).

Accordingly, even if Rayes and Iyer were combined (although there appears to be no rationale for combining), the resultant combination would not teach or suggest all of the features of Applicants' independent claim 1. Thus, Applicants submit that claim 1 is allowable over the cited art, and respectfully request that the rejection of claim 1 be withdrawn.

Independent claims 15 and 22 recite features that are substantially similar to independent claim 1, and are thus believed to be allowable for at least a similar rationale as discussed for claim 1, and others.

Dependent claims 2, 4-8, 16-19, and 23 depend (either directly or indirectly) from independent claims 1, 15, and 22 respectively, and are thus believed to be allowable for at least a similar rationale as discussed for claims 1, 15, and 22, and others.

35 U.S.C. §102 Rejection of Claim 20

Claim 20 is rejected under 35 U.S.C. §102(e) as being anticipated by Doyle. Applicants respectfully traverse the rejection.

Independent claim 20 recites, in part "analyzing at least two associations in a database accessible to the ARP collector to determine whether ARP spoofing occurs." Applicants submit that at least this feature of claim 20 is not disclosed by Doyle. The Office

Action alleges that Doyle teaches the "analyzing…" feature of claim 20 at column 9, lines 16-29. Applicants respectfully disagree.

The cited section of Doyle describes a method for detecting IP spoofing (*i.e.*, determining whether a data packet has a forged source IP address). (*See, e.g.*, Doyle: col. 8, lines 55-59). This method includes receiving a data packet and determining a MAC address and source IP address included in the packet. The MAC address and source IP address are then checked to see if they are bound to each other at the source device (*i.e.,* the device that sent the packet). If the MAC address and source IP address are bound at the source device, the data packet is determined to have a non-spoofed IP address. (Doyle: col. 9, lines 16-29).

Applicants submit that detecting IP spoofing, as described in the cited section of Doyle, is completely unrelated to detecting ARP spoofing as recited in claim 20. As discussed above, the detection of IP spoofing involves determining whether a received data packet has a spoofed IP address. In contrast, the detection of ARP spoofing involves determining whether a received data packet is a spoofed ARP reply packet sent in response to an ARP request. Since Doyle merely describes determining whether a received data packet has a spoofed IP address, rather than determining whether the received data packet is a spoofed ARP reply packet, Doyle fails to teach or suggest "analyzing… to determine whether ARP spoofing occurs" as recited in claim 20. (Emphasis added).

Applicants note that Doyle does describe sending an ARP request and receiving an ARP reply at col. 9, lines 60-64. However, Doyle simply states that the information in the ARP reply packet is used to update an ARP table; nowhere does Doyle indicate that the ARP reply packet is (or should be) checked for spoofing.

In fact, Applicants submit that Doyle necessarily assumes all received ARP replies are not spoofed. FIG. 6 of Doyle illustrates a method for detecting IP spoofing in which the source IP address included in a received data packet is checked against the ARP table discussed above. Since this method relies on the fact that the information the ARP table is genuine, Doyle necessarily assumes that the information returned in an ARP reply is also genuine; accordingly, there is no need to detect ARP spoofing. If the ARP table contained spoofed information, the method illustrated in FIG. 6 of Doyle would not be able to distinguish between a correct source IP address and a forged source IP address, thereby rendering the method useless. Since FIG. 6 of Doyle requires that all ARP replies are genuine (*i.e.*, not spoofed), Doyle necessarily fails to teach or suggest "analyzing at least two associations in a database accessible to the ARP collector to determine whether ARP spoofing occurs" as recited in claim 20. (Emphasis added).

For at least the foregoing reasons, Applicants submit that claim 20 is allowable over Doyle, and respectfully request that the rejection of claim 20 be withdrawn.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 650-326-2400.

Respectfully submitted,

/Andrew J. Lee/

Andrew J. Lee
Reg. No. 60,371

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
A2L:m4g
61400311 v1